

Notice of Allowability	Application No.	Applicant(s)	
	10/049,434	ASANO ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--
 All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to examiner's amendment authorized on 7/6/06.
2. ☒ The allowed claim(s) is/are 1-3,5-13,15,16,21,23-35 and 37.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Raymond Churchill on 7/6/06.

The claims have been amended as follows:

1. (currently amended) An information recording device for recording the information on a recording medium, comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices, operating as leaves, and a leaf key unique to each information recording device, said memory means also holding a key renewal block formed as renewal key storage data decryptable using at least one of the node key and the leaf key; and

encryption means for decrypting the key renewal block decryptable using at least one of the node key and the leaf key provided in said information recording device to calculate an encrypting key used in encrypting data to be stored in said recording medium; said encryption means encrypting the data to be stored in said recording medium using the calculated encrypting key;

said encryption means detecting, in encrypting and storing content for said recording medium, the latest usable key renewal block from key renewal blocks stored in said recording medium and from the key renewal block stored in said memory means of the information recording device itself; said encryption means encrypting the data to be stored on said recording medium using the encrypting key obtained on decrypting the detected latest usable key renewal block,-

wherein said information recording device is configured for executing processing of writing the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block stored in the memory means of the information recording device itself, in the memory means of the information recording device itself, in case the latest usable key renewal block is the key renewal block stored in the recording medium and the latest key renewal block is not as yet stored in the memory means of the information recording device itself.

4. (cancelled)

12. (currently amended) An information recording method in an information recording device adapted for recording the information for a recording medium, said information recording device holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices, operating as leaves, and a leaf key unique to each information recording device, said method comprising:

a step of detecting a latest usable one of key renewal blocks stored in the recording medium and the key renewal block stored in said memory means of the information recording device itself;

a step of decrypting the detected latest usable key renewal block, at said detection step, using at least the node key or the leaf key held in said information recording device, to calculate the encrypting key used in encrypting data stored in said recording medium; and

a step of encrypting recording data for said recording medium, using the calculated encrypting key, to store the encrypted data on the recording medium;

wherein, in case the detected latest usable key renewal block is the key renewal block stored in the recording medium and the latest key renewal block has as yet not been stored in the memory means of the information recording device itself, said detection step executes the processing of writing the latest key renewal block in said memory means of the information recording device itself.

14. (cancelled)

15. (currently amended) An information reproducing method in an information recording device adapted for recording the information for a recording medium, each of a plurality of such devices holding a node key unique to each node of a hierarchical tree structure having the plural respective information recording devices operating as leaves, and a leaf key unique to each information recording device, said method comprising:

a step of acquiring version information of an encrypting key for content being reproduced, stored in a recording medium;

a step of detecting a latest one of a key renewal block stored in the recording medium and a key renewal block stored in a memory means of the recording device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced;

a step of generating an encrypting key using at least one of the node key and the leaf key by decryption processing of a key renewal block as detected by said detection step; and

a step of decrypting cipher data stored in the recording medium using the generated encrypting key.

21. (currently amended) An information recording device for recording the information on a recording medium, each recording device comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices operating as leaves and a leaf key unique to each information recording device, said memory means also holding a key renewal block each formed as renewal key storage data decryptable using at least one of the node key and the leaf key;

encryption means for decrypting the key renewal block formed as renewal key storage data decryptable using at least one of the node key and the leaf key provided in said information recording device to calculate an encrypting key used in encrypting data to be stored in said recording medium; said encryption means encrypting the data stored in said recording medium using the calculated encrypting key; and

renewing means for comparing, in accessing the recording medium, a version of a key renewal block stored in the recording medium to that of the key renewal block owned by the information recording device itself, and for writing a key renewal block of a new version on the recording medium if the key renewal block of the new version is the key renewal block stored in the memory means of the recording device itself, and the key renewal block of the new version is not as yet stored on the recording medium,-

wherein, if a latest usable one of the key renewal blocks is the key renewal block stored on the recording medium and the latest usable key renewal block has not as yet been recorded in the memory means of the recording device itself, said renewing means writes the latest key renewal block in the memory means of the recording device itself.

22. (cancelled)

35. (currently amended) In a recording or reproducing device including a node key unique to each node forming a hierarchical tree structure having a plural number of such information recording or reproducing devices, operating as leaves, and a leaf key unique to each recording or reproducing device, said device being adapted for recording the information on a recording medium, a method for renewing an encrypting key comprising:

a detection step of detecting a latest usable one of key renewal blocks stored on the recording medium and a key renewal block stored in a memory means of the recording or reproducing device; and

a renewal step of undertaking, in case a latest version of the key renewal block is the key renewal block stored in the memory means of the information recording or reproducing device itself and the key renewal block of a new version has not been stored on the recording medium, the writing of said key renewal block of the new version on said recording medium;

wherein said renewing step further includes a step of undertaking, in case the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block owned by the information recording or reproducing device itself is the key renewal block stored on said recording medium, and the latest key renewal block has as yet not been stored in the memory means of the information recording or reproducing device, including a processing of writing said latest key renewal block in the memory means of the recording and/or reproducing device itself, and

wherein the latest usable key renewal block is decryptable using at least one of the node key and the leaf key to determine the encryption key.

36. (cancelled)

2. The following is an examiner's statement of reasons for allowance.
The present invention is directed to: (i) an information recording device which selects a latest key renewal block between a key renewal block stored on the recording device and a key renewal block stored on a recording medium, derives an encryption key using the latest key renewal block, encrypts information to be recorded using the derived encryption key, and

records the encrypted information on the recording medium; and (ii) an information reproducing device which derives a decryption key using a key renewal block stored on the recording medium, and decrypts information from the recording medium using derived decryption key. More specifically, independent claims 1, 12, 21 and 35 identify the uniquely distinct features: if the key renewal block stored on the recording device is not the latest key renewal block, the key renewal block stored on the recording medium will be stored on the recording device. The closest prior art, Lotspiech (6,609,116), discloses an information recording device which selects a latest key renewal block between a key renewal block stored on the recording device and a key renewal block stored on a recording medium, derives an encryption key using the latest key renewal block, encrypts information to be recorded using the derived encryption key, and records the encrypted information on the recording medium. However, the key renewal block stored on the recording medium of Lotspiech can only be as current as the key renewal block stored on the recording device, and therefore, will not be stored on the recording device.

Independent claims 7, 15 and 28 are directed to an information reproducing device which selects a latest key renewal block between a key renewal block stored on the information reproducing device and a key renewal block stored on a recording medium, derives a decryption key using

the latest key renewal block, and decrypts information from the recording medium using derived decryption key. The closest prior art, Lotspiech (6,609,116), discloses an information reproducing device which only uses a key renewal stored on the recording medium to derive a decryption key for reproducing information from the recording medium. Another prior art, Ishiguro (5,796,839), discloses using a decryption key with a correct version for decrypting information from a recording medium; however, Ishiguro does not disclose using a latest key renewal block to derive the decryption key.

The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

MD
7/6/06


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100